Advisory Alert

Alert Number: AAA2023628 **Date:** June 28, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Netgear	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Redhat	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Netgear**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Netgear has released security updates addressing multiple vulnerabilities affecting their products. An improper remote server certificate validation security vulnerability exists in RAX50 routers. And a re-authentication command injection security vulnerability exists in RAX30 routers; if an attacker has your Wi-Fi password or an Ethernet connection to a device on your network as well as the admin login and password to your network the exploit can be carried out. Netgear recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	RAX50 firmware version prior to 1.0.15.128 RAX30 firmware version prior to 1.0.11.96_2_HOTFIX
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000065699/Security-Advisory-for-Pre-Authentication-Command-Injection-on-the-RAX30-PSV-2023-0046 https://kb.netgear.com/000065668/Security-Advisory-for-Improper-Remote-Server-Certificate-Validation-on-the-RAX50-PSV-2023-0019

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1390, CVE-2023-23455, CVE-2023-31436, CVE-2020-36694, CVE-2021-29650, CVE-2022-3566, CVE-2022-4269, CVE-2022-45884, CVE-2022-45885, CVE-2022-45886, CVE-2022-45887, CVE-2022-45919, CVE-2023-1079, CVE-2023-1380, CVE-2023-1637, CVE-2023-2124, CVE-2023-2194, CVE-2023-23586, CVE-2023-2483, CVE-2023-2513, CVE-2023-31084, CVE-2023-31436, CVE-2023-32233, CVE-2023-32269, CVE-2023-33288, CVE-2023-1382, CVE-2023-2002, CVE-2023-2156, CVE-2023-2162, CVE-2023-2269, CVE-2023-28410, CVE-2023-3006, CVE-2023-30456)
Description	Suse has released security updates addressing multiple vulnerabilities affecting their products. Exploitation of the most severe vulnerabilities could lead to Denial of Service, Use-after-free condition, Memory leak, Race condition. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Basesystem Module 15-SP4 Development Tools Module 15-SP4 Legacy Module 15-SP4 openSUSE Leap 15.4 openSUSE Leap Micro 5.3 SUSE Enterprise Storage 7 SUSE Linux Enterprise Desktop 15 SP4 SUSE Linux Enterprise High Availability Extension 15 SP2, 15 SP4, SUSE Linux Enterprise High Performance Computing 12 SP4, 15 SP2, 15 SP2 LTSS 15-SP2, 15 SP4 SUSE Linux Enterprise Live Patching 12-SP4, 15-SP2, 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 12 SP4, 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP4, 15 SP2, 15 SP4 SUSE Linux Enterprise Workstation Extension 15 SP4 SUSE Manager Proxy 4.1, 4.3 SUSE Manager Retail Branch Server 4.1, 4.3 SUSE Manager Server 4.1, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232660-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232651-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232653-1/

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2700, CVE-2023-1281, CVE-2023-32233)
Description	Redhat has released security updates addressing multiple vulnerabilities affecting their products. **CVE-2023-2700** - A vulnerability exist in libvirt, caused due to repeatedly querying an SR-IOV PCI device's capabilities that exposes a memory leak caused by a failure to free the virPCIVirtualFunction array within the parent struct's g_autoptr cleanup. **CVE-2023-1281** - A use-after-free vulnerability was found in the traffic control index filter (tcindex) in the Linux kernel. A local attacker could cause a use-after-free problem, leading to privilege escalation. **CVE-2023-32233** - A use-after-free vulnerability was found in the Netfilter subsystem of the Linux kernel when processing batch requests to update nf_tables configuration. A local user (with CAP_NET_ADMIN capability) could use this flaw to crash the system or potentially escalate their privileges on the system. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 8.8 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:3852 https://access.redhat.com/errata/RHSA-2023:3853 https://access.redhat.com/errata/RHSA-2023:3822

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.